



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,947	11/27/2001	Rasmus Relander	P 282888	8087
909	7590	11/17/2006	2000937US/LT/HER	
PILLSBURY WINTHROP SHAW PITTMAN, LLP			EXAMINER	
P.O. BOX 10500			ZIA, SYED	
MCLEAN, VA 22102			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/993,947

Applicant(s)

RELANDER ET AL.

Examiner

Syed Zia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 16 August 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

This office action is in response to arguments filed on August 16, 2006. Original application contained Claims 1-29. Applicant did not submit any amendment. Therefore, presently pending claims are 1-29.

### *Response to Arguments*

Applicant's arguments filed on August 16, 2006 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-29 applicants argued that the system of cited prior art (CPA) [Samarakoon et al. (Encrypted Video over TETRA), Lipmaa et al. (Comments to NIST concerning AES Modes of Operation: CTR-Mode Encryption), and Kramer et al. (US Patent 6,658,027)] “*merely teaches to reduce the data rate to compensate for the reduced transmission capacity due to the inserted synchronization frames. As a result, the inserted synchronization frames in the solution of Samarakoon do not increase the reproduction delay*”, *and,*” as recited in independent claim 1.

This is not found persuasive. The system of cited prior art teaches system that uses a frame insertion synchronization techniques to reduce the data rate to maintain overall transmission rate and using of describe fly-wheeling technique to avoid loss of synchronization due to dropped data packets to provide synchronization to end-to-end encrypted data, thus

Art Unit: 2131

counting only the frames not marked as extra frames in the number of received frames. the frames that satisfies the criteria that represent the silent interval, thereby determining conditions when a frame need to be deleted or inserted and compensates rate mismatches between near and far end devices. [Samarakoon: Fig. 2; Fig. 3, Fig. 2, IV, feedback from output of block cipher to IV, and Pg. 2 “Frame Insertion techniques”] [Lipmaa et al. Pg. 2 “operation” and “Advantages of CTR Mode”], and [[Kramer: Fig. 2 “IP Socket” input, and Col. 9 lines 46-60; “insert an additional silence frame...”].

As a result, cited prior art does implement and teach system that relates to a method and apparatus for maintaining end-to-end synchronization on a telecommunications connection.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and dependent claims. Accordingly, rejections for Claims 1-29 are respectfully maintained.

***Claim Rejections - 35 USC § 112***

1. Applicant's arguments with respect to the 112 rejections of claims 8, and 14 have been fully considered and are persuasive. The 112 rejections of these claims have been withdrawn.

***Claim Rejections - 35 USC § 103***

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. In regards to claims 1, 7, 13, and 22 note that the preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

4. **Claims 1-18, 22-26, and 29 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Samarakoon et al. (Encrypted Video over TETRA) in view of Lipmaa et al. (Comments to NIST concerning AES Modes of Operation: CTR-Mode Encryption) and further in view of Kramer et al. (US Patent 6,658,027).

Art Unit: 2131

5. **In regards to claim 1**, Samarakoon et al. teach a system and methods for synchronization of an encrypted video stream over TETRA. Specifically, Samarakoon et al. teach:

- A method for maintaining end-to-end synchronization on a telecommunications connection transmitting data in frames in real time [Pg. 2 “Frame Insertion Techniques” paragraph 1, Fig. 2] and using synchronized end to end encryption [Fig. 2; Fig. 3], wherein an IV vector value corresponding to a received frame and used in decrypting the frame is defined on the number of frames received at the receiving end of the telecommunications connection [Fig. 2, IV, feedback from output of block cipher to IV], and wherein at least a part of the telecommunications connection is a packet-switched connection [Abstract, Tetra, Dropped Packets], the method comprising:
  - One or more extra frames [are added] to the frame string being transmitted. [Synchronization frame is added and marked as a synchronization frame; Pg. 2 “Frame Insertion techniques”]

What Samarakoon et al. do not teach is that the reproduction delay is increased, or that only frames not marked as extra frames are counted.

Lipmaa et al. teach CTR-Mode Encryption, a block cipher [Fig. 1]. It is well known in the art that the Nonce of CTR-Mode [Pg. 1 Usage Scenarios] is equivalent to what is to an IV in other block ciphers.

It would have been obvious to one of ordinary skill in the art to use CTR mode as the block cipher of Samarakoon et al. Samarakoon et al. specify the use of a block cipher, but not a

Art Unit: 2131

specific block cipher. Lipmaa et al. teach the block cipher mode CTR, and in addition a number of advantages, including software efficiency, hardware efficiency, provable security, etc. [Pg. 2 “Advantages of CTR Mode”] The combination of Samarakoon et al. and Lipmaa et al. teach the limitation “*counting only the frames not marked as extra frames in the number of received frames*” because upon receiving a new IV in CTR mode, the counter is reset to the new IV [Lipmaa et al. Pg. 2 “operation”]. Thus, the frame that is sent containing the IV in Samarakoon et al. is not counted by the counter.

What is still not taught by the combination of Samarakoon et al. and Lipmaa et al. is increasing the reproduction delay of the data being transmitted.

Kramer et al. teach a system and methods for jitter buffer management. Note that the jitter correction is done at an IP boundary [Fig. 2 “IP Socket” input] Specifically, Kramer et al. teach:

- Increasing the reproduction delay of data being transmitted by adding one or more extra frames to the frame string being transmitted [Col. 9 lines 46-60; “insert an additional silence frame...”]

It would have been obvious to one of ordinary skill in the art, when performing jitter control on a real time transmission as in Kramer et al., to use the inserted frames of Samarakoon et al. as the silence frame of Kramer et al. First, one of skill in the art would recognize that jitter control is important in real-time communication, and Kramer et al. present a system and methods to implement jitter control. Since both Kramer et al. and the combination of Samarakoon et al. implement their respective functions by adding an additional frame, it would be obvious to use the same added frame to perform both functions to reduce communication overhead.

Art Unit: 2131

6. **In regards to claim 7**, the combination of Samarakoon et al., Lipmaa et al., and Kramer et al. teach:

- Means for adjusting the reproduction delay arranged to increase the reproduction delay of the data being transmitted [Samarakoon et al. Fig. 2 “Control Unit,” Kramer et al. Fig. 2 “Jitter Buffer Manager”] by adding one or more extra frames to the frame string being transmitted [Kramer et al. Col. 9 lines 46-60 “insert an additional silence frame”]
- Means for defining on the basis of the number of received frames an IV vector value corresponding to a frame received at the receiving end of the telecommunications connection [Lipmaa et al. Fig. 1 “ctr+n-2”] and used in decrypting the frame [Lipmaa et al. Fig. 1 “ $M_{n-1} = E_K(ctr+n-2) \text{ xor } C_{n-1}$ ”]
- The means for adjusting the reproduction delay are arranged to mark the frames to be added to increase the reproduction delay as an extra frame [Samarakoon et al. Pg. 2 “Frame Insertion Techniques” synchronization frame] whereby the means for defining the initialization vector value are arranged to count only the frames not marked as extra frames in the number of received frames [Inherent. A new IV resets the counter, hence the frame with the IV would not increment the counter]

7. **In regards to claim 13**, the combination of Samarakoon et al., Lipmaa et al., and Kramer et al. teach:

- A network element [Samarakoon et al. Pg. 2 Transmitter] for maintaining end-to-end synchronization on a telecommunications connection transmitting data in frames in real time [Samarakoon et al. Pg. 2 “Frame Insertion Techniques”]



paragraph 1, Fig. 2] and using synchronized end to end encryption [Samarakoon et al. Fig. 2; Fig. 3], wherein an IV vector value corresponding to a received frame and used in decrypting the frame is defined on the number of frames received at the receiving end of the telecommunications connection [Samarakoon et al. Fig. 2, IV, feedback from output of block cipher to IV], and wherein at least a part of the telecommunications connection is a packet-switched connection [Samarakoon et al. Abstract, Tetra, Dropped Packets], the network element being arranged:

- To increase the reproduction delay of the data being transmitted [Samarakoon et al. Fig. 2 “Control Unit,” Kramer et al. Fig. 2 “Jitter Buffer Manager”] by adding one or more extra frames to the frame string being transmitted [Kramer et al. Col. 9 lines 46-60 “insert an additional silence frame”]

8. **In regards to claim 22**, the combination of Samarakoon et al., Lipmaa et al., and Kramer et al. teach:

- A network element [Samarakoon et al. Fig. 3] for use in a telecommunications connection transmitting data in frames in real time [Samarakoon et al. Pg. 2 “Frame Insertion Techniques” paragraph 1, Fig. 2] and using synchronized end to end encryption [Samarakoon et al. Fig. 2; Fig. 3], wherein at least a part of the telecommunications connection is a packet-switched connection [Kramer et al. Fig. 2 “IP Socket”], in which case the reproduction delay of the data being transmitted can be increased by adding one or more extra frames to the frame

string being transmitted [Kramer et al. Col. 9 lines 46-60 “insert an additional silence frame”], the network element being arranged:

- To define on the basis of the number of received frames an IV vector value corresponding to a received frame [Lipmaa et al. Fig. 1 “ctr+n-2”] and used in decrypting the frame [Lipmaa et al. Fig. 1 “ $M_{n-1} = E_K(ctr+n-2) \text{ xor } C_{n-1}$ ”]
- When the frames added to increase the reproduction delay are marked as extra frames, to count in the number of received frames only the frames that are not marked as extra frames [Inherent. A new IV resets the counter, hence the frame with the IV would not increment the counter] added to increase the reproduction delay [Col. 9 lines 46-60; “insert an additional silence frame...”]

9. **In regards to claim 2**, it is taught that the reproduction delay is increased in the receiving end of the packet-switched connection. [Kramer et al. Col. 9 lines 46-60]

10. **In regards to claims 3, 9, 16, and 24** the invention of Kramer et al. is specifically drawn towards IP [Kramer et al. Fig. 2 “IP Socket”]

11. **In regards to claims 4, 10, 17, and 25** the telecommunications connection belongs to the TETRA system [Samarakoon et al.; Abstract; TETRA...]

12. **In regards to claims 5, 11, 15, and 23** Samarakoon et al. teach “The TETRA system uses a synchronization technique known as frame stealing to provide synchronization to end-to-end encrypted data ... however the frame stealing process degrades the quality of video and is not suitable for transmission of secure video.” One of ordinary skill in the art would recognize that in the synchronization scheme of Samarakoon, it would be obvious to do the

Art Unit: 2131

synchronization in a stolen speech block for audio, as Samarakoon teaches is already done for audio.

13. **In regards to claims 6, 12, 18, and 26** the encryption is done using a key stream segment [Lipmaa et al. Fig. 1 “ctr, ctr+1...”] generated using the IV [Lipmaa et al. “usage scenario” “ctr ... encodes the number nonce\*2<sup>64</sup> ... Typically, one transmits C along with a string which encodes the nonce]

14. **In regards to claims 8 and 14**, the reproduction delay is adjusted in the receiving entity [Kramer et al. Col. 9 lines 46-60]

15. **In regards to claim 29**, Samarakoon et al. teach the network element can be a mobile station [Samarakoon et al. Introduction Sentence 3 “one mobile station to another”]

16. **Claims 20-21 and 28 are rejected under 35 U.S.C. 103(a)** as being unpatentable over the combination of Samarakoon et al. as applied to claims 13 and 22 above, and further in view of the ESTI (Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 1: General network Design).

17. **In regards to claims 20 and 28**, the combination of Samarakoon et al. teaches all the limitations of claims 13 and 22 above. What the combination of Samarakoon et al. does not explicitly teach is that the network element is a base station.

The ESTI teaches many standard configurations for TETRA. Specifically, they teach in 4.3.1 example 3 that the MS/LE is directly connected to TETRA, which is directly connected to a PDN/DTE.

Art Unit: 2131

It would have been obvious to one of ordinary skill in the art, given a network configuration as in ESTI, to have the network element be a base station. The network element in question in Samarakoon et al. concerns only the TETRA elements of the network, hence it would be obvious to consider the transmitter/receiver to reside at the TETRA boundary. One of ordinary skill in the art would recognize, given the network configuration as in case 3 of ESTI, that the network element would reside in the base station, as the base station provides the gateway between TETRA and the PDN.

18. **In regards to claim 21**, the invention of Kramer et al. teach that the jitter correction is done at the IP boundary [Fig. 2 “IP Socket”] hence given network arrangement 4.3.1 example 3 [ESTI 4.3.1 example 3] the jitter correction i.e. the packet insertion would be done at the PDN/TETRA gateway.

19. **Claims 19 and 27 are rejected under 35 U.S.C. 103(a)** as being unpatentable over the combination of Samarakoon et al. as applied to claims 13 and 22 above, and further in view of Uhlirz (Concept of a GSM-based Communication System for High-Speed Trains).

20. **In regards to claims 19 and 27**, the combination of Samarakoon et al. teaches all the limitations of claims 13 and 22. What the combination of Samarakoon et al. does not teach is that the network element is a TETRA dispatcher workstation.

Uhlirz teaches that the one of the present communication needs of a High-Speed train communication system is “a dispatcher or local coordinator stay in touch with the personnel at the train station ... [which] is of type point-to-multipoint (trunked radio application).” [Uhlirz, II.A “Profile of present communication needs” bullet 2]

It would have been obvious for one of ordinary skill in the art to take the communication system taught in claims 25, 26, 17, and 18 – which is a trunked radio system by definition (the TR in TETRA standing for trunked radio) – and to use it in the role Uhlriz as a dispatcher workstation.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SZ

November 03, 2006

Syed Zahid  
Syllabus Examiner